SECTION FIVE.
Possibilities of Applying LegalTech Tools in Legal Communication

Self Sovereign Identity

Michal Tabor

1. Electronic Identification

Identification and authentication of the users to the online services is one of the key needs of Internet business and electronic transactions. Electronic identification was established in European Union as legal definition in the eIDAS regulation.

> *'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person; (article 3 eIDAS)*

The eIDAS Regulation founded general requirements for identification means complying with levels of assurance, and general needs to recognize and accept electronic identification in public online services. Electronic identification is widely used by public services but was not so widely adopted by business. Private systems in general onboard and register users on their systems each time by their own methods, some services ceded authentication to large solution providers, in particular Google, Apple and Microsoft. For several years, work has been underway to build Self-Sovereign Identity (SSI) technology that allows much more than using person identification data as defined in eIDAS. SSI enables the use of own user identity attributes in the manner in an independent way, where no one particular operator takes actions in the identification process. Moreover, European Commission takes action to force law online services to accept SSI identification in all their services. Your identity is determined by many attributes, some of which are permanent, such as your date of birth, while others, such as your home address, may change. Each of the identity attributes has its origin, e.g. name, surname, date of birth and parents' data come from the register of civil status, while the ID number from the register of personal documents. The concept of SSI is that individual identity attributes can be collected by their holder from different sources, while their use and which ones will be used is decided by the holder himself.

Most solutions for electronic identification used now are based on two models: centralized and federated. In a centralized identity management model, you have to onboard to each service separately and you use individual credentials (login and password) to access to each service (e.g. office, bank, e-store, boking platform). In the federation model, the attributes and authentication mechanism are maintained by a single identity provider and accepted by other systems – this model is the basis for functioning in notified electronic identification means in the EU and also is used for solutions like Login with Google/Apple/Facebook. In both of these models (centralized and federated), a services are in possession of user identity data; manage them and allow authentication. SSI assumes that it is the user himself who manages the attributes of his identity and implements the authentication process, based on the IT solution he/she is in control.[1]

As indicated above, multiple attributes may be associated with an individual's identity (user), m.in.: first name, last name, date of birth, adulthood, residence, identification number, *tax number*, *email*, phone number, and much more. Each of these attributes can be used in specific actions, but very rarely you need to use them at once. Within SSI, the attribute holder selects the attributes (and only those) that they want to use, and authenticates their own possession, without the need for external systems.

Example:

To illustrate an SSI concept, you might want to describe it in the following usage example:

1) The holder launches on his smartphone an application constituting his wallet for managing an self-sovereign identity. As in an electronic signature, this wallet is associated with a public and private key that allows the holder to collect and use individual attributes.
2) The holder must confirm their wallet with the first identification service, which will allow him to assign the first attributes that allow his identification in other systems. These attributes will be assigned to the public key that was previously generated in the wallet.
3) Each use of identities and attributes is preceded by a system that asks for that identity. Such a system must show that it is entitled to ask

1 Christopher Allen, 'The Path to Self-Sovereign Identity' (*Life With Alarcity*, 25 April 2016) <http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html> accessed 21 February 2021; See 'Self-Sovereign Identity' (The Moxy Tongue, 9 February 2016) <http://www.moxytongue.com/2016/02/self-sovereign-identity.html> accessed 21 February 2021.

questions and should provide a list of expected attributes. The holder will have the right to choose the ones that he decides to present;

4) The holder, presenting his attribute by signing it, proves that he owns it. Once authenticated, the holder will be able to complete the collection of attributes they have, e.g. education, driving privileges, or information about their funds in their account.

The SSI concept is implemented on the basis of open algorithms and standardized data formats and commonly recognized cryptographic algorithms. Standardization allows the user to choose the technologies and applications by which the above processes will be described, and in particular will allow the maintenance of cryptographic keys and support for a wallet. The implementation of the SSI allows the identified person to control what information he/she makes available to the system and to prevent central systems from collecting access to information about where and when his or her identity was used. The whole is complemented by the fact that identifiers in independent identity solutions do not need (or should not be) immutable identification numbers. Multiple Identifiers can be assigned to a single user, and their structure should prevent operations from being tracked.

Self-sovereign identity is based on technical standards developed by W3C standards organisation and involves a number of standardisation initiatives, including *Verifiable Credentials*(VC) and [2] *Decentralized Identifiers*(DID).[3]

The verifiable credentials technology allows the unambiguous identification of the relationship between natural persons, legal entities and other objects (car, dog, house, other object), in a way in which the relationship is unambiguous, the credential is confirmed by trusted source and the credential can only be used by a person authorized to do so.

2 'Verifiable Credentials Data Model 1.0. Expressing verifiable information on the Web' (*W3C*, 19 November 2019) <https://www.w3.org/TR/vc-data-model/> accessed 21 February 2021.

3 'Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations' (*W3C*, 3 August 2021) <https://www.w3.org/TR/did-core/> accessed 3 August 2021.

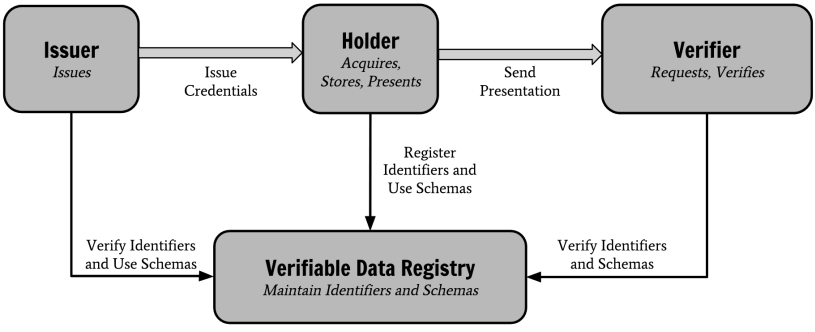
Example:

A typical verifiable credential shows examples of relationships:

1) Michael [owns] a car.
2) Agnes [obtained a master's degree in economics] from the University of Oxford.

Verifiable Credentials technology not only unambiguously describes the relationships between individual entities, but also allows them to be used in accordance with the rules set out in the verifiable credential itself. The relationship resulting from verifiable credentials is best illustrated in the following figure:

Figure 1. Roles and information flow



Source: Verifiable Credentials Data Model 1.0, § 1.2.

Each Verifiable Credential uniquely identifies its publisher (a trusted source), the holder, and the objects that are described in the verifiable credential. The issuer must be trusted and verifiable, which is implemented on the basis of cryptographic technologies, electronic signatures and seals or Blockchain technologies. The publisher, when creating a Verifiable Credential, indicates its *Holder* and specifies the cryptographic method that will be used to authenticate it. Using this technology, the holder will have direct access to the contents of the verifiable credential, e.g. put it in his wallet, but will also be able to use it. The use of the Verifiable Credential is called a presentation. The presentation of the Verifiable Credential shall include the entire credential and the digital signature of the holder. Verifiable Credential contain in the body information how holder is authenticated, so in the process of presentation authentication of the

holder can by verified by the verifier. The whole scheme needs for proper functioning a public register, which due to its characteristics is most often implemented on the basis of DLT (distributed ledger technologies). DLT enable the operation and use of distributed registries. A distributed register is [4]defined as a ledger that is shared by a set of DLT nodes and synchronized between DLT nodes using a consensus mechanism.[5]

Ensuring the clarity of relationships in SSI solutions is based on Decentralized Identifiers (DID) that unambiguously and uniquely identify a specific person, object, or explicitly Verifiable Credential. Also note that DID itself (as an identifier) is not an identity. The reason is that DID is a unique, random string of alphanumeric characters, under the control of the user, while only the user has a private cryptographic key, stored in a digital wallet, which he can use to confirm any operation (based on the DID ID). DID also does not contain any other identity attributes, such as first name, last name, and so on. Thus, with DID, the user can simply prove that he controls this alphanumeric number, but no longer his identity. On the other hand, a verifiable credential that can be issued to a DID holder also contains a set of identity attributes.

Example:

Each of the objects mentioned above, i.e. Michael, car, Agnies, University of Oxford will have a DID assigned in verifiable credentials. When a user shares their verifiable credentials with someone, they generate a DID proof of ownership (digitally signing with a PRIVATE DID key), and the recipient can verify who has identity attributes in the Verifiable Credential.

2. *Distributed Confirmations*

The entire Decentralized Identifiers solution can use various technologies to secure integrity and authenticity, in particular digital signature technologies, but blockchain-based technologies, in particular *distributed* DLT, are the most natural technologies for a distributed environment. Based on a distributed registry, DID does not require a centralized enrolment

4 For a broader overview of DLT technology, see Electronic Communication chapter by Anna Zalesińska and Dariusz Szostek.

5 ISO/TC 307, 'ISO 22739:2020 Blockchain and distributed ledger technologies' (July 2020).

system, allowing the deployment of decentralized public key infrastructure (DPKI) and decentralized key management system (DKMS),[6] tools independent of a single trust service provider, a single hierarchy,and maintaining the independence of subsequent certificate publishers.

Each Distributed DID is bound to a document (DID *Document).* In fact, this document is a Verifiable Credential placed in a verifiable registry, while the use of a distributed DLT provides certainty of access and security of the integrity of such a registry. At the same time, the DID Publisher has the ability to manage the lifecycle of such an identifier, such as changing its status, invalidating or updating it.

The independent identity mechanism described earlier uses Verifiable Credentials to describe the identity attributes of the wallet holder. Verifiable Credentials are placed directly in the data portfolio or accessible through a Verifiable Registry. Each identification is in fact a verifiable credential presentation service, while all objects related to that identity are uniquely identified by decentralized identifiers, while shared data based on identifiers can be accessed through the registry and DLT.

Example:

On the main *smartphone platforms, there* are already production implementations of the wallet used to store Verifiable Credentials and Distributed Identifiers, these applications implement the above-mentioned processes of cryptographic key generation for the holder, provide the functions of saving Verifiable Credentials and Distributed Identifiers. All available solutions allow you to identify both the system asking for identity and the use of identity attributes in electronic identification, as well as to confirm the transaction.

It is planned that the European Commission will introduce an obligation for all service providers in the EU to identify and use independent identity mechanisms by all service providers in the EU as part of the 2021-2023 review of eIDAS.[7] The aim of this action is to provide a universal (for all citizens of UE) identification scheme, allowing for proof of identity, both in public administration systems and in private systems. To

6 Alexander Papageorgiou, Antonis Mygiakis, Konsantinos Loupos and Thomas. Krousarlis, 'DPKI: A Blockchain-Based Decentralized Public Key Infrastructure System' (2020 Global Internet of Things Summit (GIoTS) Dublin, June 2020).

7 Alex Preukschat, 'Understanding the European Self-Sovereign Identity Framework (ESSIF) – Daniël Du Seuil and Carlos Pastor – Webinar 32' <https://ssimeetup.org/understanding-european-self-sovereign-identity-framework-essif-daniel-du-seuil-carlos-pastor-webinar-32/> accessed 21 February 2021.

this end, each Member State will be required to provide services to the public *to obtain Verifiable Credentials of its identity, and at the same time any online service provider, whether public or* private, will be required to accept the identification thus carried out in its services. As part of the development and testing of capabilities, the EC has launched the "EU Login" application, which allows testing to be carried out in the framework of projects carried out in the Connecting Europe *Facility* (CEF) programme.[8]

8 CEF Digital, 'eID' <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID> accessed: 21 February 2021.